고성능 침입탐지 및 대응 시스템의 구현 및 성능 평가

김 형 주† · 박 대 철††

요 약

최근 정보통신기반이 급속히 발달하고 사용자가 늘어남에 여러가지 사이버 공격이 늘어나고 있다. 침해사고를 예방하고 효과적인 대응방법이 마련된 침입탐지시스템들은 저속 환경에서의 실시간 분석에 적합하도록 설계되고 구현되었기 때문에, 증가하는 트래픽 양을 처리하는데 어려움이 있다. 또한, 기가비트 이더넷(Gigabit Ethernet) 환경과 같은 고속 네트워크 환경이 현실화 되므로 대용량의 데이터를 처리할 수 있는 효과적인 보안 분석 기법들이 필요하다. 본 논문에서는 고속 네트워크 환경에 필요한 침입탐지 및 그 대응 방법에 위한 고속 침입탐지 메커니즘 적용 시스템을 제안한다. 이는 패킷 헤더 기반의 패턴 매칭 기능과 시스템 커널 영역에서 수행되는 패킷 데이터 기반의 패턴 매칭 기능을 통해서, 고속 네트워크 환경에 적합한 침입탐지 메커니즘을 제안하며, 시스템의 성능을 기존 운용 시스템과 비교 분석함으로써, 제안한 침입탐지 메커니즘이 트래픽 처리성능면에서 최대 20배까지 우수했다.

Implementation and Performance Evaluation of High-Performance Intrusion Detection and Response System

Hyeong-Ju Kim† · Dae-Chul Park††

ABSTRACT

Recently, the growth of information infrastructure is getting faster and faster. At the same time, the security accidents are increasing together. We have problem that do not handle traffic because we have the Intrusion Detection Systems in low speed environment. In order to overcome this, we need effective security analysis techniques that can processed data of high-capacity because high speed network environment. In this paper we proposed the Gigabit Intrusion Detection System for coordinated security function such as intrusion detection, response on the high speed network. We suggested the detection mechanism in high speed network environment that have pattern matching function based packet header and based packet data that is proceeded in system kernel area, we are shown that this mechanism was excellent until maximum 20 times than existing system in traffic processing performance.

키워드 : 기가비트 이더넷(Gigabit Ethernet), 보안사고(Security Accident), 침입탐지시스템 (Intrusion Detection System), 고속 네트워크 (High Speed Network)

1. 서 론

고속 네트워크 보급확산에 따라 대용량 데이터의 송수신은 침입탐지시스템의 적용 환경에도 많은 영향을 미치게 되었다. 또한, 인터넷의 발전과 더불어 네트워크 상에서의 침입 시도가 갈수록 증가되고 다변화됨으로써, 기존의 저속 침입탐지 기법에 대한 변화를 요구하고 있다. 다시 말해서, 갈수록 고속화 되고 대용량화 하는 네트워크 환경과 보다 다양해 지는 침입 시도에 적절히 대응하기 위해서는, 보다 빠른 시간 내에 많은 데이터를 분석할 수 있는 기법이 요구된다. 그러나, 현재의 대다수 침입탐지시스템들은 고속 이더넷(Fast Ethernet) 환경에서의 실시간 분석에 적합하도록 설계되고 구현되었기 때문에, 갈수록 증가하는 트래픽 양을 처리하는데 어려움이 있다. 즉, 기가비트 이더넷(Gigabit Ethernet) 환경과 같은 고속 네트워크 환경이 현실화 되고 있기 때문에, 이를 수용할 수 있는 보안 분석 기법들이 요구되고 있다. 따라서, 본 논문에서는 고속 네트워크 환경에서의 침입탐지 및 대응 기능을 제공하기 위한 기가비트 침입탐지시스템을 제안한다. 이는 기가비트 이더넷 환경과 같은 고속 네트워크 환경에 적합한 탐지 메커니즘으로써, FPGA Logic을 이용한 패킷 헤더 기반의 패턴 매칭 기능과 시스템 커널 영역에서 수행하는 패킷 데이터 기반의 패턴 매칭 기능을 통한 고속의 침입탐지 기능을 제공한다. 또한, 하드웨어적으로 처리되는 네트워크 패킷 수집 및 유해 트래픽에 대한 고속차단 기능을 제공한다. 즉, 본 논문에서 제안하고 있는 기가비트 침입탐지시스템은 다양한 침입을 보다 빨리 탐지하고 대응하기 위한 시스템이며, 이

† 정 회 원 : 정보통신연구진흥원 선임연구원
†† 정 회 원 : 한남대학교 정보통신공학과 교수
논문접수 : 2004년 1월 28일, 심사완료 : 2004년 2월 9일

를 효율적으로 수행하기 위한 시스템 구조를 갖는다.

본 논문의 구성은 2장에서 침입탐지시스템에 대한 기존의 연구 결과 및 동향들에 대해서 살펴보고, 3장에서 제안된 기가비트 침입탐지시스템의 구조와 이에 요구되는 구성요소 및 수행 기능에 대해서 기술한다. 4장에서는 제안된 시스템의 구현 및 성능 평가 결과에 대해서 기술하며, 마지막으로 5장은 결론 및 향후 연구과제를 기술한다.

2. 관련 연구

현재 침입탐지시스템은 공공기관에서 높은 예산을 집행하고 있을 정도로 그 중요성이 높이 인식되고 있으며, 국내외적으로 여러 제품들이 연구 개발되고 있다. 그러나, 기존의 침입탐지시스템은 방대한 데이터 분석에 따른 성능 문제 및 탐지오류 등의 많은 문제를 가지고 있다[1].

현재의 침입탐지시스템이 지니고 있는 기술적 한계 즉, 문제점은 무엇보다도 패킷 분실율 및 침입 탐지율과 같은 침입탐지시스템의 성능 문제이다. 성능은 꾸준히 여러 개발자들에 의해서 개선되고는 있으나, 성능 개선은 무엇보다도 중요한 해결 과제로 대두된다. 또한, 점점 고속화, 대용량화되어 가는 네트워크 환경으로 중요성이 더욱 부각되고 있다. 여러 working group에서 이러한 성능상의 요구를 수용하기 위한 연구가 진행되고 있으며, 실제로 많은 상업 제품들이 개발되었다[2-6]. 대부분 100Mbps이하 환경에서의 침해대응 성능을 보증하고 200Mbps까지 동작 가능하며, 일부 제품은 기가비트 환경까지 지원하고 있다. 이러한 기술들은 고속 트래픽 모니터링과 메모리 관리, 데이터베이스 관리 및 커널의 컨트롤이 가능해야 하며, 그만큼 좋은 인프라가 앞선 기술을 만들어 내고 있다고 볼 수 있다. 그러나, 이들에 대한 성능 분석 결과가 불분명하고 명확한 속도 향상 기법은 제시되고 있지 못하다.

따라서, 본 논문에서는 이러한 성능 개선의 관점에서 시스템을 설계하고, 이를 통한 고속 침입탐지 및 대응 기능을 제공하고자 한다. 이 기능은 기본적으로 패킷 수집 및 유해 트래픽에 대한 차단 기능 등을 전담하고, 침입탐지 기능을 부분적으로 수행할 수 있는 FPGA Logic과 커널 영역에서의 침입탐지 모듈을 통해서 수행된다.

3. 기가비트 침입탐지시스템의 설계

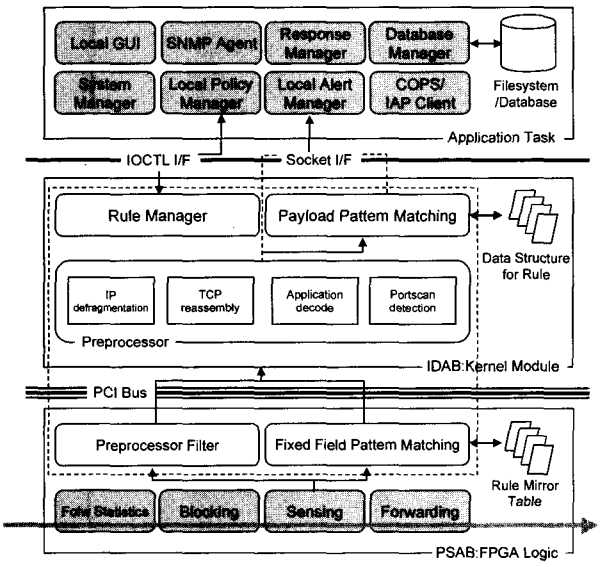
본 장에서는 기가비트 이더넷(Gigabit Ethernet) 환경과 같은 고속 네트워크 환경에서의 고속 침입탐지 및 대응 기능을 제공하기 위한 시스템 구조를 설계하고, 이에 필요한 시스템 구성 요소 및 기능에 대해 설명한다.

3.1 기가비트 침입탐지시스템의 구조

제안된 기가비트 침입탐지시스템은 기본적으로 대규모 네트워크 환경에서의 침입탐지 및 대응을 위한 시스템으로써, 개개 보안 영역에 대한 보안 정책을 가지고 동작한다. 즉, 네트워크 보안 제어를 위한 하부 시스템으로 동작하며, 고속 침입탐지 수행 결과는 상위의 보안 정책 제어를 위한 관리 시스템으로 전달되고, 이로부터 침입 경보에 대한 제어를 전달 받게 된다.

여기에서, 고속 침입탐지 기능을 갖는 기가비트 침입탐지 시스템의 전체적인 블록 구조는 (그림 1)과 같다. 그림에서와 같이, 제안된 시스템은 크게 PSAB(Packet Sensing and Blocking) 블록, IDAB(Intrusion Detection and Analyzing Block) 블록과 Application Task 블록으로 구성된다.

우선, Application Task 블록은 시스템에 대한 전체적인 관리 및 제어를 제공하며, 크게 System Manager, Local Policy Manager, Local Alert Manager 및 COPS/IAP Client 등으로 구성된다. 각 기능 블록들을 통해서, Application Task 블록은 하부 블록으로부터의 경보 데이터 처리 및 상위 관리 시스템과의 연계를 통한 정책 관리, 각종 시스템 정보 관리 등을 수행한다.



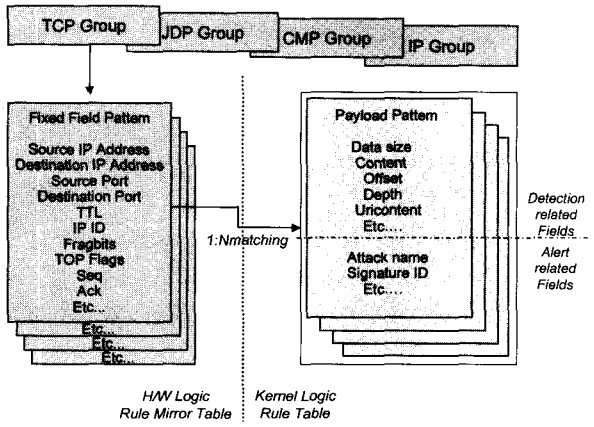
(그림 1) 기가비트 침입탐지시스템의 구조

다음으로, IDAB 블록은 커널 모듈 기반의 고속 침입탐지 기능을 수행하며, 이를 위한 기능 블록들로 구성된다. 이 침입탐지 기능은 크게 패킷 데이터 기반의 패턴 매칭 기능(Payload Pattern Matching)과 전처리 기능(Preprocessor)으로 구분되며, 하부 FPGA Logic에서의 처리 결과를 기반으로 수행된다. 상기에서, 패킷 데이터 기반의 패턴 매칭은 규칙 기반으로 수행되며, 전처리 기능은 어플리케이션 레벨의 디코딩 및 특정 유형의 침입 유형을 탐지하게 된다. 이 탐지 결과는 소켓 인터페이스를 통해서, 상위 Application Task 블록으로 전달된다.

마지막으로 PSAB 블록은 FPGA Logic을 통한 고속의 패킷 처리 기능을 수행함으로써, 침입탐지를 위한 일차적인 역할을 담당하게 된다. 즉, 전처리 필터링(Preprocessor Filtering)과 패킷 헤더 기반의 패턴 매칭(Fixed Field Pattern Matching)을 수행함으로써, PCI 버스를 통한 패킷 전송 부하를 최소화하게 된다. 이외에도, 네트워크 패킷에 대한 Blocking과 Sensing, Forwarding 기능을 수행하며, 처리된 패킷에 대한 통계 정보를 제공한다.

3.2 침입탐지 규칙 구성 및 적용

제안된 시스템은 IDAB 블록의 커널 모듈과 PSAB 블록의 FPGA Logic을 통해서 규칙 기반의 침입탐지 기능을 수행한다. 따라서, 하드웨어와 소프트웨어로 구분된 탐지 모듈을 통한 침입탐지 기능을 수행하기 위해서는 적절한 탐지 규칙 구성 및 적용이 필요하다.



(그림 2) 침입탐지 규칙 구성

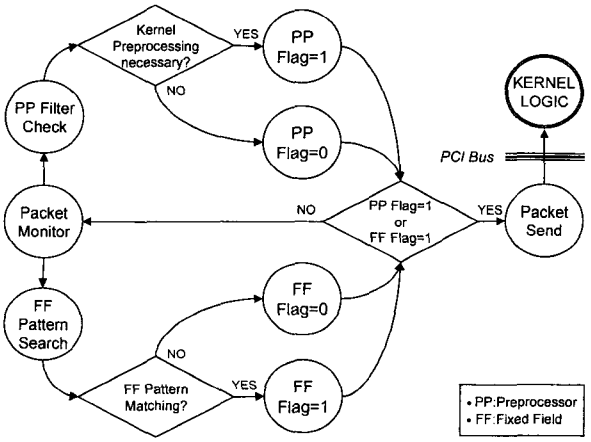
(그림 2)는 제안된 시스템에 적용되는 침입탐지 규칙의 구성을 보인다. 그림에서와 같이, 적용될 침입탐지 규칙들은 프로토콜에 따라 크게 4개의 그룹으로 구분되며, TCP와 관련된 침입 규칙, UDP와 관련된 침입 규칙, ICMP와 관련된 침입 규칙, 그리고 IP와 관련된 침입 규칙으로 구성된다. 다시, 각 그룹에 속하는 침입 규칙들은 패킷 헤더와 관련된 검색 필드들로 구성된 고정 필드 패턴(Fixed Field Pattern)들과 패킷 데이터와 관련된 검색 필드들로 구성된 페이로드 패턴(Payload Pattern)들의 조합으로 구성된다[10]. 여기에서, 동일한 고정 필드들을 갖는 침입 규칙들에 대한 검색 성능 향상을 위해서, 각 고정 필드 패턴들은 자신에 속하는 여러 개의 페이로드 패턴과 연결될 수 있다. 즉, 고정 필드 패턴과 페이로드 패턴은 일대다의 관계로 연결되어 구성된다.

상기에서, 고정 필드 패턴들은 지정된 위치에서의 패턴 매칭이 가능하기 때문에 FPGA Logic을 통한 고속 처리가 가능하나, 페이로드 패턴들은 패킷 페이로드의 가변적인 위치와 길이에 따라서 처리되어야 하는 복잡성 때문에 커널 모듈에서 처리된다. 무엇보다도, 위와 같은 침입탐지 규칙의 구성은 FPGA Logic에서의 매칭된 결과만이 커널 모듈로 전달하도록 하기 때문에, 커널 모듈에서의 수행 부하를 최소로 해 준다.

3.3 고속 침입탐지 메커니즘

제안된 시스템의 고속 침입탐지 기능은 FPGA Logic을 통한 하드웨어적인 수행과 커널 영역에서의 탐지 기능 수행을 통해서 제공된다. 즉, 유입되는 패킷에 대한 PSAB 블록에서의 일차적인 처리와 IDAB 블록에서의 이차적인 처리를 통해서 최종적인 침입 유무를 판단함으로써, 고속 침입탐지 기능을 제공하고자 하였다. 따라서, 제안된 시스템의 고속 침입탐지 메커니즘은 PSAB 블록의 FPGA Logic과 IDAB 블록의 커널 모듈을 통한 성능 향상에 초점을 둔다.

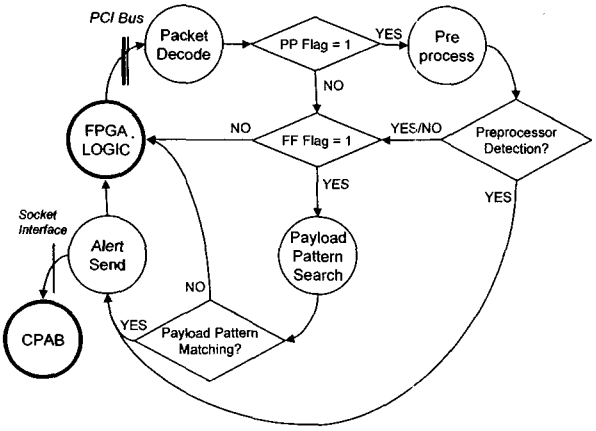
우선, PSAB 블록의 FPGA Logic은 전처리 필터링과 고정 필드 패턴 매칭을 수행하기 위해서, (그림 3)과 같은 패킷 처리 메커니즘을 수행한다. 우선, 전처리 필터링은 유입 패킷에 대한 커널 영역에서의 전처리 필요 유무를 점검함으로써, 전처리 플래그(PP Flag)를 설정하게 된다. 다음으로, 고정 필드 패턴 매칭은 유입 패킷에 부합하는 고정 필드 패턴이 존재하는지 여부를 점검함으로써, 고정 필드 플래그(FF Flag)를 '1'로 설정하게 된다. 위의 수행 결과, 전처리 플래그가 '1'이거나, 고정 필드 플래그가 '1'인 경우에만 상위 모듈로 해당 수행 결과를 전달하게 된다. 즉, 이와 같은 패킷 처리 메커니즘을 통해서, 상위로 전달되는 패킷의 양을 일차적으로 줄여주는 역할을 수행한다.



(그림 3) FPGA Logic에서의 패킷 처리 메커니즘

상기의 FPGA Logic에서의 수행 결과를 바탕으로, IDAB 블록의 커널 모듈은 패킷 데이터 기반의 패턴 매칭과 전처리 기능을 수행한다. (그림 4)는 이에 대한 IDAB 블록 내의 패킷 처리 메커니즘을 보인다. 우선, PSAB 블록으로부터의 전처리 플래그 정보가 '1'로 설정되어 있다면, 해당 패킷에 대한 전처리를 수행하며, 이에 따른 경보 메시지 생성

및 어플리케이션 디코딩을 수행하게 된다. 다음으로, 고정 필드 플래그가 '1'로 설정되어 있다면, 해당 고정 필드에 속하는 페이로드 패턴들을 검색함으로써, 침입 유무를 판단하게 된다. 검색 결과, 해당 패턴이 존재한다면 상위의 Application Task로 경보 메시지를 전달하게 된다. 무엇보다도, IDAB 블록 내에서의 패킷 처리 메커니즘은 시스템의 커널 영역에서 수행되기 때문에, 기존 어플리케이션 영역에서 수행되던 기능에 비해 보다 나은 성능 향상을 제공하게 된다.



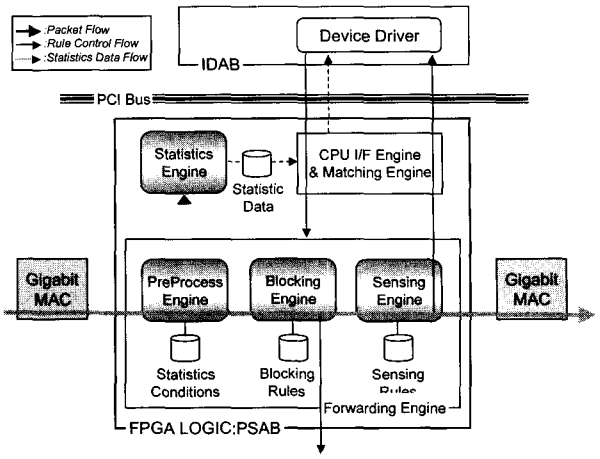
(그림 4) Kernel Logic에서의 패킷 처리 메커니즘

제안된 시스템은 FPGA Logic과 커널 영역에서의 패킷 처리를 수행하는 상기의 고속 침입탐지 메커니즘을 통해서 보다 빠른 침입탐지 기능을 제공할 수 있다.

3.4 침입대응 기능

제안된 시스템의 PSAB 블록은 위에서 기술된 침입탐지 기능 이외에, 침입에 대한 대응으로써의 유해 트래픽에 대한 차단 기능 등을 지원한다. (그림 5)는 이를 제공하기 위한 FPGA Logic에서의 패킷 흐름도를 보인다. 그림에서, 유해 트래픽에 대한 차단 기능은 Blocking Engine을 통해서 제공되며, 부수적으로 유입 패킷에 대한 각종 통계 데이터 생성 및 패킷 필터링을 수행하는 PreProcess Engine, 이를 바탕으로 통계 데이터를 저장하고 제공하는 Statistics Engine, 상위 IDAB 블록으로 수집 패킷을 전달하기 위한 Sensing Engine, 선로 상의 패킷을 고속으로 통과시키기 위한 Forwarding Engine 등으로 구성된다.

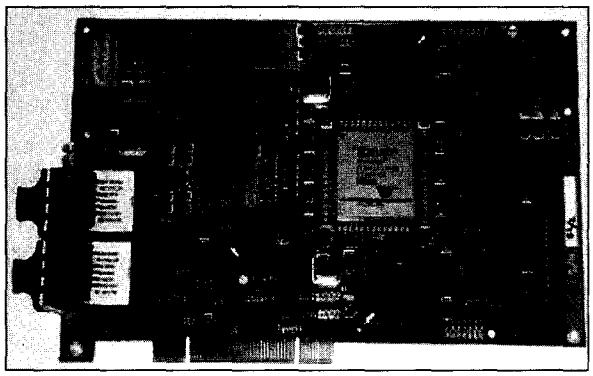
(그림 5)에서와 같이, PSAB 블록은 양 네트워크 사이에서 브릿지 형태로 설치되기 때문에, 유해 트래픽에 대한 직접적인 차단 기능을 제공할 수 있다. 또한, 이와 같은 차단 기능을 통해서 침입탐지를 위한 패킷량을 줄여줄 뿐만 아니라, 유해 트래픽으로부터 해당 네트워크 및 시스템들을 보호할 수 있다.



(그림 5) FPGA logic에서의 패킷 흐름도

4. 시스템 구현 및 성능 평가

본 논문에서 제안한 기가비트 침입탐지시스템은 기존의 침입탐지시스템이 지닌 성능 문제를 개선하고자 노력하였으며, 프로토타입 시스템을 구현하였다. 기본적으로 프로토타입 구현은 리눅스 머신 상에서 구현되었으며, 이는 커널 상에서의 작업 편의성에 기인한다. 또한, FPGA Logic 구현 및 시험을 위해서, (그림 6)과 같은 프로토타입 보드를 제작하였다. 제작된 프로토타입 보드는 32bit/33Mhz의 PCI 인터페이스를 지니며, FPGA Logic을 위해서, Xillinx XC2V 4000-5FF1152C 칩을 사용하였다.



(그림 6) 시스템 프로토타입 보드 제작

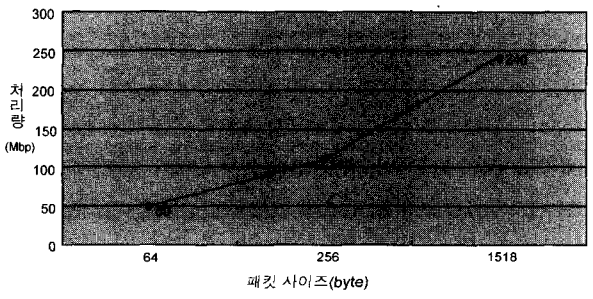
(그림 6)의 프로토타입 시스템에 대한 성능 측정은 IXIA 계측기를 통해서 수행하였으며, 계측기를 통해서 생성된 유해 트래픽의 처리 능력에 중점을 두고 측정하였다. 이는 정상 트래픽의 경우, FPGA Logic에서의 일차적인 필터링 수행으로 인해서, 커널 영역까지의 전체적인 처리 성능을 측정하기 곤란하기 때문이다. 즉, 유해 트래픽의 유입시, 이를 처리하는 기능 모듈들의 전체적인 성능을 측정하고자 하였다.

〈표 1〉 세부 성능 평가 결과표

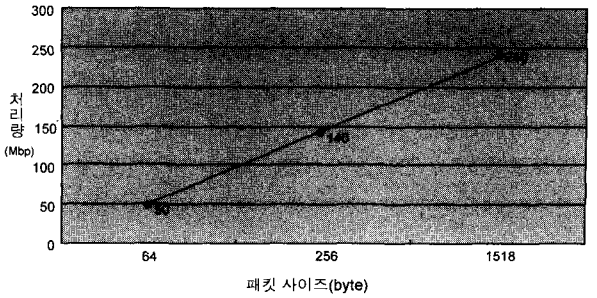
측정 상황 \ 패킷사이즈(Byte)	64	256	1518
TCP 유해 트래픽	30Mbps	100Mbps	230Mbps
	50Mbps	110Mbps	240Mbps
UDP 유해 트래픽	40Mbps	140Mbps	240Mbps
	50Mbps	140Mbps	240Mbps
ICMP 유해 트래픽	40Mbps	130Mbps	240Mbps
	50Mbps	130Mbps	240Mbps

상기와 같은 방식으로 전체적인 침입탐지 기능의 패킷 처리 성능을 측정하기 위해서, 계측기의 Tx 카운트와 FPGA Logic 및 커널 영역에서 수행한 패킷 카운트가 일치하는 동안, 계측기의 Tx 트래픽을 증가시켜 최대 Tx 트래픽을 찾고자 하였다. 또한, 각각의 프로토콜별 64byte, 256byte, 1518byte 크기의 유해 트래픽을 발생시킴으로써, 프로토콜별 처리 성능 및 패킷 사이즈별 처리 성능을 측정하고자 하였다. 이를 통한 성능 평가 결과표는 <표 1>과 같다. 표에서 각 프로토콜별로 상위의 측정 결과는 FPGA Logic과 커널 영역에서 100% 처리된 경우의 트래픽 양을 나타내며, 하위의 측정 결과는 커널 영역에서의 손실은 발생하나, 처리될 수 있는 최대 한계치를 나타낸다. 즉, 유해 트래픽의 유입부터 이를 처리하는 FPGA Logic과 커널 영역에서의 패킷 처리까지 수행될 수 있는 패킷 처리 성능의 한계치를 나타낸다.

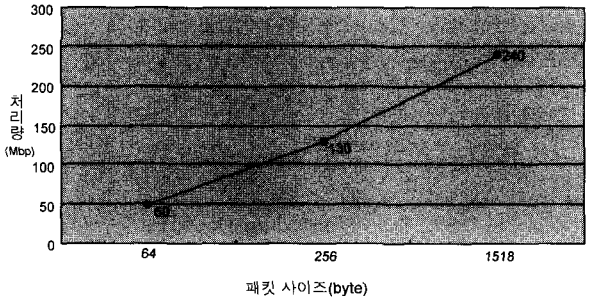
(그림 7), (그림 8), (그림 9)는 세부 성능 평가 결과를 바탕으로, 각 프로토콜 별 패킷 처리 성능을 나타낸 것이다. 각 프로토콜 별로의 패킷 처리 성능은 거의 차이를 보이지 않으나, 패킷 사이즈에 의해 큰 차이를 보인다. 즉, 1518byte 사이즈 트래픽의 경우, 240Mbps까지 처리하나, 64byte 사이즈 트래픽의 경우는 50Mbps까지 처리함을 알 수 있다. 그러나, 이는 100% 유해 트래픽을 기반으로 측정한 결과이므로, 실제 환경의 경우, FPGA Logic을 통한 필터링이 일차적으로 수행될 경우, PCI 인터페이스를 통한 커널 영역으로의 패킷 전달량은 현저히 줄어들 것이라 판단한다. 즉, 일반 트래픽의 경우, FPGA Logic을 통한 기가급의 처리가 가능하며, 일차적으로 유해하다고 판단된 패킷에 대해서는 50~240Mbps까지 처리가 가능하다.



(그림 7) TCP 패킷 처리 성능



(그림 8) UDP 패킷 처리 성능



(그림 9) ICMP 패킷 처리 성능

<표 2>는 성능 측정 결과를 바탕으로 기존 운용 시스템과의 성능 비교를 나타낸다. 성능 비교를 위한 타 시스템으로는 일반적으로 널리 알려진 snort-2.0.0 버전을 선택하였다[5]. 성능 비교는 IXIA 계측기를 통해서 수행하였으며, 1Giga의 정상 트래픽을 백 트래픽으로 전송하는 상태에서의 탐지율을 측정하였다. 즉, 임의로 생성된 1Giga의 백 트래픽 상에 탐지율 측정을 위한 유해 트래픽을 총 1,000,000씩을 전송하였다. 유해 트래픽은 프로토콜 및 패킷 사이즈에 따라 각기 다른 속도로 전송하였으며, 이는 제안된 시스템의 최대 처리 성능을 기반으로 전송하였다. 가령, 64byte의 TCP 유해 트래픽에 대한 탐지율을 비교하기 위해서는 50Mbps의 속도로 1,000,000개의 유해 트래픽을 전송하였으며, 이에 대한 탐지 결과를 천 단위로 표시하였다. 아래의 표에서, 상위의 측정 결과는 제안된 시스템에서 발생된 경보의 수를 나타내며, 하위의 측정 결과는 snort에서 발생된 경보의 수를 나타낸다. 표에서 보는 바와 같이, 제안된 시스템은 거의 모든 패킷을 처리하고 이에 대한 경보를 생성한 반면, snort의 경우는 최저 5%에서 최대 40%까지의 경보 생성율을 보인다.

〈표 2〉 타 시스템과의 성능 비교표

측정 상황(Alerts) \ 패킷사이즈(Bytes)		64	256	1518
TCP 유해 트래픽	제안시스템	999,000	999,000	999,000
	비교시스템	75,000	134,000	400,000
UDP 유해 트래픽	제안시스템	999,000	999,000	999,000
	비교시스템	51,000	50,000	100,000
ICMP 유해 트래픽	제안시스템	999,000	999,000	999,000
	비교시스템	54,000	70,000	170,000

상기의 결과표에서 보는 바와 같이, 제안된 시스템은 일반적으로 어플리케이션 형태로 동작하는 시스템에 비해 최대 20배의 성능 우위를 가지고 있음을 알 수 있다. 즉, 제안된 시스템은 유해한 트래픽의 경우에만 커널 영역까지 전달하고 처리하기 때문에, CPU 상에서의 처리 부하를 최소화 하였다. 이는 결과적으로 고속 네트워크 환경에서의 대규모 데이터를 고속으로 처리할 수 있도록 도와준다.

5. 결론 및 향후 연구과제

본 논문에서는 기가비트 이더넷(Gigabit Ethernet) 환경과 같은 고속 네트워크 환경에서의 고속 침입탐지 및 대응 기능을 제공하기 위한 기가비트 침입탐지시스템 구조를 설계하고, 이에 필요한 시스템 구성 요소 및 기능에 대해서 설명하였다. 무엇보다도, 자체 제작한 하드웨어 보드를 통해서 패킷을 수집하고, FPGA Logic을 통한 일차적인 패킷 처리와 커널 영역에서 최종적인 패킷 분석을 통해서 안정적인 고속 침입탐지 기능을 제공하고자 하였다. 또한, 유해 트래픽에 대한 차단 기능을 하드웨어적으로 처리함으로써, 패킷 처리에 대한 고속화를 추구함과 동시에 네트워크를 통한 침해 행위로부터의 피해를 최소화하고자 하였다.

앞으로는 이에 대한 여러 시험을 통해서 나오는 문제점들을 보완하고, 보다 나은 침입탐지 및 대응 기능을 제공하기 위한 기법들을 연구해 나가고자 한다. 즉, 보다 고속화 되어가는 네트워크 환경에서의 보다 나은 성능 향상을 위해서, 보다 많은 부분을 FPGA Logic을 통해서 처리하는 방안을 고려하고자 한다. 이러한 연구는 보다 많은 데이터를 고속으로 처리함으로써, 간혹 놓치기 쉬운 여러 위협으로부터 자신의 네트워크를 보호하는데 도움을 줄 것이다.

참 고 문 헌

[1] Kruegel, C., Valeur, F., Vigna, G. and Kemmerer, R. "Stateful intrusion detection for high-speed networks," In *Proceedings of the IEEE Symposium on Security and Privacy*, pp.266-274, 2002.

[2] ISS., "RealSecure Gigabit Network Sensor.," http://www.iss.net/products_services/enterprise_protection/rsnetwork/gigabitsensor.php, September, 2002.

[3] Symantec, "ManHunt.," http://enterprisesecurity. Symantec.com/products/products.cfm? ProductID=156, 2002.

[4] CISCO, "CISCO Intrusion Detection System. Technical Information," CISCO, November, 2001.

[5] M. Roesch, "Snort-Lightweight Intrusion Detection for Networks," In *Proceedings of the USENIX LISA '99 Conference*, pp.100-106, November, 1999.

[6] Marcus Ranum, "Burglar Alarms for Detecting Intrusions," NFR Inc., 1999.

[7] Thomas Ptacek and Timothy Newsham, "Insertion, Evasion, and Denial of Service : Eluding Network Intrusion Detection," Secure Networks Inc., 1998.

[8] H. Debar, M. Dacier and A. Wespi, "Research Report Towards a Taxonomy of Intrusion Detection Systems," Technical Report RZ 3030, IBM Research Division, Zurich Research Laboratory, Jun., 1998.

[9] S. Kumar and E. Spafford, "A pattern matching model for misuse intrusion detection," In *Proceedings of the 17th National Computer Security Conference*, pp. 11-21, Oct., 1994.

[10] W. Richard Stevens, *TCP/IP Illustrated Volume I : The Protocols*, Addison Wesley, 1994.

김 형 주

e-mail : hjookim@iita.re.kr

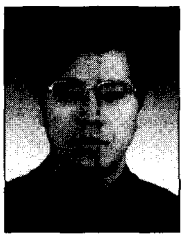
1982년 경북대학교 전자공학과(학사)

1987년 동아대학교 전자공학과(석사)

1987년~1997년 한국전자통신연구원 선임연구원

1998년~현재 정보통신연구진흥원 선임연구원

관심분야 : 고속통신망 성능평가, 네트워크 보안 등



박 대 철

e-mail : daechul@hannam.ac.kr

1977년 서강대학교 전자공학과(학사)

1985년 미국 Univ. of New Mexico 전기공학과(석사)

1989년 미국 Univ. of New Mexico 전기공학과(박사)

1977년~1982년 국방과학연구소 연구원

1989년~1993년 한국전자통신연구원 선임연구원

1993년~현재 한남대학교 정보통신공학과 교수

관심분야 : 통신신호처리, 디지털 워터마킹 등